www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-1, Apr- 2013
Research Paper

Int. J. Sci. Res. in Network Security and Communication

ISSN: 2321-3256

A Novel Security Based Model for Wireless Mesh Networks

Shivlal Mewada[1*], Umesh Kumar Singh[2] and Pradeep Sharma[3]

[1,2]*Institute of Computer Science, Vikram University, Ujjain - India*
[3]*Department of Computer Science, Govt. Holkar Science College, Indore*

Received: 08 March 2013 | Revised: 22 March 2013 | Accepted: 12 April 2013 | Published: 10 May 2013

***Abstract*— Wireless mesh network (WMN) is a new emerging field with its potential applications in extremely unpredictable and dynamic environments. WMN has the feather of self-organization, distributed structure. WMN is going to address the internet provision to users at low cost anytime from anywhere, as it allows a fast, easy and inexpensive network deployment. However, they are far from mature for large-scale deployment in some applications due to the lack of the satisfactory guarantees on security. In the wireless mesh networks, management model is one of the most important secure problems. We propose a security based model for wireless mesh network which be adapted by large groups according to network characteristics.**

Keywords*—*WMNs; MANET; Security; Security model; Protocols

I. INTRODUCTION

All WMNs represent a new network concept and therefore introduce new security specifics. Here, we describe these specifics by giving an overview of the primary differences between WMNs and two well-established infrastructure based technologies: cellular networks and the Internet.

The major difference between WMNs and cellular networks - besides the use of different frequency bands (WMNs usually make use of unlicensed frequencies) - concerns the network configuration: In cellular networks, a given area is divided into cells and each cell is under the control of a base station. Each base station handles a certain number of mobile clients that are in its immediate vicinity (i.e., communication between the mobile clients and the base station is single-hop) and it plays an important role in the functioning of the cellular network; the entity that plays an equivalent role in WMNs would be the Wireless Host Spots [1, 2, 3, 4].

However, whereas all the security aspects can be successfully handled by the base station in cellular networks, it is risky to rely only on the Wireless Host Spots to secure a WMN, given that the communications in WMNs are multi-hop. Indeed, centralizing all security operations at the WHS would delay attack detection and treatment and therefore would give the adversary an undeniable advantage. Furthermore, multi-hopping makes routing in WMNs a very important and necessary functionality of the network; and like all critical operations, an adversary may be tempted to attack it. The routing mechanism must thus be secured.

Multi- hopping has also an important effect on the network utilization and performance. Indeed, if the WMN is not well-designed, a Transmit Access Points (TAPs) that is several hops away from the WHS would receive a much lower bandwidth share than a TAP that is next to it. This leads to severe unfairness problems, and even starvation [5]; it thus can be used by an adversary to disturb the functioning of the WMN.

In WMNs, the wireless TAPs play the role that is played, in the classic (wired) Internet, by the routers. Given that wireless communications are vulnerable to passive attacks such as eavesdropping, as well as to active attacks such as Denial of Service (DoS), WMNs are subject to all these attacks whose effects are amplified by the multi-hop aspect of the communications.

Another primary difference between the Internet and WMNs is that, unlike Internet routers, the TAPs are not physically protected. Indeed, they are most often in locations that are accessible to potential adversaries, e.g., deployed on rooftops or attached to streetlights. The absence of physical protection of the devices makes WMNs vulnerable to some serious attacks. Indeed, one very important requirement regarding the Transmit Access Points - for the concept of mesh networks to remain economically viable - is their low cost that excludes the possibility of strong hardware protection of the devices (e.g., detection of pressure, voltage, or temperature changes) [1,6]. Therefore, attacks such as tampering, capture or replication of Transmit Access Points are possible and even easy to perform. New security challenges are mainly due to the multi-hop wireless communications and by the fact that the Transmit Access Points are not physically protected. Multi-hopping delays the detection and treatment of the attacks, makes routing a critical network service and may lead to severe unfairness between the TAPs, whereas the physical exposure of the TAPs allows an adversary to capture, clone or tamper with these devices.

II. CHARACTERISTICS OF WMNS

WMN is a wireless co-operative communication infrastructure between massive amounts of individual wireless transceivers (i.e. a wireless mesh). This type of

*Corresponding Author: *Shivlal Mewada*

infrastructure is decentralized, relatively inexpensive, and very reliable and resilient, as each node need only transmit as far as the next node. Nodes act as repeaters to transmit data from nearby nodes to peers that are too far away to reach, resulting in a network that can span large distances, especially over rough or difficult terrain [7].

WMNs are extremely reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbors simply find another route. Extra capacity can be installed by simply adding more nodes. Mesh networks may involve either fixed or mobile devices as shown in Figure 1. The principle is simple: data will hop from one device to another until it reaches a given destination. One advantage is that, like a natural load balancing system, the more devices the more bandwidth becomes available. Since this wireless infrastructure has the potential to be much cheaper than the traditional networks, many wireless community network groups are already creating WMNs.

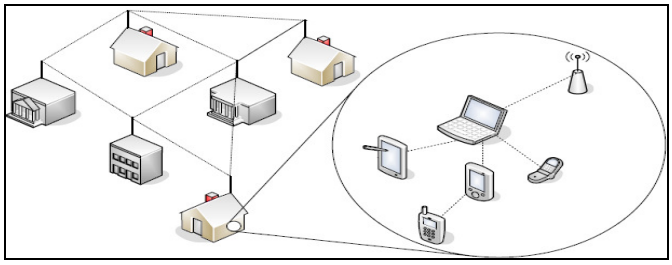

Figure: 1 an Example of WMNs [5]

Constrains: There are five main constraints in every current wireless networks including wireless Wi-Fi, WMN, MANET.

- *CPU:* large computations on the end nodes are slow, as computing power of the processor is small.
- *Battery:* total energy resource is very limited and it is not desirable to use the device for large computations and transmissions.
- *Scalability:* the current wireless networks act poorly when the networks enlarged in both aspects of members and computation.
- *Mobility:* mobile devices expose great pressure on the convergence and ability of hand-over to the networks.
- *Bandwidth:* bandwidth in amongst the mobile nodes is also limited.

III. SECURITY MANAGEMENT

Security is critical in the process of deploying and management of Wireless Mesh Networks (WMNs). In WMNs, like in MANETs (Mobile Ad Hoc networks), security is easy to compromise due to specific characteristics of these networks:

- There is a shared wireless medium among the network nodes; this means that channels are vulnerable
- The topology of the network changes dynamically making it more difficult to trace malicious actions

The possible attacks may occur at routing protocol or MAC protocol levels. Routing attacks include: advertising routing updated for DSR and AODV protocols, packet forwarding (which may act without changing the routing tables, but still leading packets on the routing path to a different destination), impersonating a legitimate node and misbehaving, or creating a wormhole and shortcutting the normal flows.

Naouel Ben Salem presents in [1], starting from a simplified view of a WMN, three primary security operations, namely: detecting corrupt TAPs, securing multihop routing and assuring fairness. The approach draws from the security paradigm, and adds to it the challenges encountered due to the specific characteristics of WMNs: multi-hop network, power constraints and mobility. Several verification scenarios are discussed: authentication of a mobile client (MC) in relation to a TAP, mutual authentication of TAPs and/or the WHS, and integrity verification. Symmetric key cryptography is preferred over asymmetric cryptography on time and complexity reasons, and a solution for message authentication, based on Message Authentication Codes (MACs), is presented. Based on these assumptions, counter measures are enumerated for attacks mainly grouped according to their target actions: corrupting TAPs, Multihop routing attacks, and attacks that disturb the fairness in the network. The architecture of a WMN is a little simplified, as it does not consider the possibility of multiple routers with gateway functions (WHS) for "internet" access, and thus it does not catch more complex interactions going on in the network. Finally, an example is given, of vehicular networks, where the concept of WMNs is not fully (correctly) exploited, by fixing WHS on telephone posts along-side the road, and considering vehicles, mobile TAPs. This would have better fit the model if the vehicles had been mobile clients switching from a static TAP to another as they move along the road.

IV. Security Challenges of WMNs

Certain verifications need to be performed as related to interaction between mobile clients and Wireless Access Points (also known as TAPs, or wireless mesh routers):

1. Mobile Client authentication; this can be anything of the already existent techniques (drawn from wired networks, or from mobile telephony):

- Use of predefined shared secret
- Employment roaming system
- or of a temporary billing account
- Public key cryptography primitives – unsuitable because not energy efficient
- Attacker can continuously ask the MC to compute or verify signatures –> MC battery drainage

Public key cryptography primitives for this case are unsuitable because they are not energy efficient. Since a mobile node is power sensible, an attacker can exploit this and can continuously ask the mobile node to compute or verify signatures. This, in time will lead mobile client battery

drainage, and consequently will take the node out of the network.

2. Mutual authentication of network nodes. This is done in two phases:

At initialization phase, when WMN is first deployed (re-initialization–if reconfiguration of the network needed). Asymmetric key cryptography can be performed here since TAPs (Wireless Access Points) and WHS (Wireless Hot Spots, also known as Wireless Gateways) are energy rich. For this to be done, the managing operator assigns a certified public/private key pair to TAPs and WHS. The mobile client can use the TAP's certified public key for authentication during session establishment.

During session established by the MC Public key cryptography to authenticate the sender/receiver for every packet is a heavy process and is not suitable for Wireless Mesh network architecture. The alternative is symmetric key cryptography. This is employed by using session keys or long-term shared keys that were originally loaded into the nodes. Message Authentication Codes (MAC) is then computed for messages between intermediate TAPs on the basis of symmetric keys predefined for each neighboring TAPs pair

3. Integrity verification .This is done either end-to-end, or at each intermediate TAP, or both. A solution could be for nodes to establish a symmetric key with the MC (mobile client). The message is protected by the MC using the MAC scheme as defined in [1]

Detection of Corrupt TAPs: Physical capture of a TAP is not necessary. Distant hacking can be employed for this. The WHS (Wireless Hot Spots or Wireless Gateway) is assumed to be physically protected. Thus it can be used to handle/store critical cryptographic data (instead of the TAPs). Four main attacks can be performed on TAPs:

1. Simple removal/replacement of a TAP. This may be done to modify the topology of the network to the benefit of the adversary.
2. Access the internal state of the captured device without changing it. This is a passive attack and is done with the purpose of retrieving secret data (public/private key pair, symmetric keys shared with neighbouring TAPs or WHS) from the TAP. A solution to counteract this type of attack is periodic erasure and reprogramming of TAPs.
3. Modify the internal state of the TAP. The purpose of this attack can be to modify the routing algorithm with the final goal of changing the network topology. A combat solution is presented by Seshadri et al in [8].

4. Clone the captured device and install replicas in strategic places in the network. The purpose of this attack is to inject false data or disconnect parts of the WMN.

Secure Multi-hop Routing: Due to the multi-hop nature of the WMNs, the routing mechanisms are essential to the smooth, effective running of the network. Compromising this area could seriously damage network performance. It is therefore of utmost importance that it is kept secure. Possible threats that a WMN can succumb to if its routing mechanisms are not secure:

- Deteriorating performance of the network by increasing the length of communication paths between the WHS and the TAPs.
- Isolation of a TAP which could inadvertently mean the isolation of a geographic region (which connects to the network by means of the isolated TAP).
- Redirecting traffic through a particular TAP in order to monitor the traffic.
- Further methods for attacking the routing mechanisms by means of packet injection are:
- Black hole - Creating forged packets to impersonate a valid mesh node simultaneously dropping packets (attracting packets is done by advertising routes as low-cost) [7/9].
- Grey hole - Creating forged packets to (i) attack and selectively drop, routes or (ii) inspect network traffic.
- Worm hole - Routing control messages and replaying them in different locations in the network to severely disrupt routing.
- Route error injection - disrupting routing by injecting forged route error message in order to break mesh links.

The last attack (route error injection) in comparison to the other routing attacks has higher exploitability because it does not require detailed knowledge.

Vehicular networks: So far, we have assumed the TAPs to be static. Vehicular networks represent a special case of WMNs that consists of a set of mobile TAPs (represented by the cars) and of roadside WHSs. The spectrum of applications offered by a vehicular network is wide ranging: It goes from safety related applications such as reporting important events (e.g., an accident) or traffic optimization through cooperative driving (e.g., deviate the traffic to avoid a traffic jam) to payment services (e.g., electronic toll collection) and location-based services (e.g., targeted marketing) [1].

ARSA: Yanchao Zhang et al, in ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks, [9], presents an architecture which eliminates the need for establishing bilateral roaming agreements and real-time interactions between potentially numerous WMN operators. The architecture is based on the assumption that the Wireless Mesh Network operates under an operator control and replaces the home/foreign-domain model usually encountered in GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunication System) or Mobile IP networks which involves the existence of a home domain where a user is registered and account information is kept, and which is contacted by foreign domains every time authentication or payment settling is needed.

The paper is mainly focused on security issues relating to network access (as opposed to infrastructure

security – believed to be taken care of by the operators, and application security – achieved via high-layer security mechanisms like IPSec) such as: router – client AKA, client – client AKA, location privacy, signalling authentication and service availability. It further explains how security is achieved for this using identity-based cryptography (IBC) as an alternative to certificate-based cryptography (CBC).

ARSA entitles the existence of brokers which issue universal *passes* to users, who then can roam freely in the domains of the WMN operators who have made agreements with brokers (far less in number then WMN operators). Authentication and key agreement (AKA) between a client and a WMN domain would then only involve a local interaction, which spares a lot of overhead.

The whole concept is built across trust domains, which, in ARSA, are managed by brokers or by WMN operators. These offer passes as follows:

- Router passes (R-Passes) are issued by a WMN operator to routers in its domain
- Client passes (C-Passes) are issued by a broker to registered clients
- Temporary client passes (T-Passes) are issued by a WMN operator to clients roaming in its domain

V. PROPOSED SECURITY BASED MODEL

The proposed model will be carried out in the following steps:

A. Theoretical Structure: The theoretical structure would be designed to accommodate Attack Model and security based Model. In the Attack Model part, the project will start with some most well-defined and important attacks including passive attack, Denial of Services and replaying attack (active attacks). The defined attack model would be used to analyze the security level of the proposed security based model, that is, if the proposed model coped well corresponding to the attack model, then high level of security is achieved. If possible, more attacks will be measured in order to strengthen the security level of proposed security based model. A few new definitions and parameters should be developed in the system initialization stage and a few new features should be added to the common cryptographic methods to accommodate the WMN environment. Definitions of node joining, leaving, and scalability would be given to address the Wireless mesh network environment at this stage as well.

B. Security Model: There are three levels of security model would be targeted including security model protocols for

- Mesh Routers pattern,
- Mesh Clients pattern,
- Mesh Router and Clients pattern addressing the different status of entities within wireless mesh networks.

Mesh routers Pattern: because the mesh routers form the backbone for the entire networking and have reasonable high input/output capability, top level of security is required. Additional, the Mesh routers model has the excellent tolerance of computation overhead and most routers are static making the Trusted Third Party (CA) possible. Thus, complicated cryptographic methods, such as Public Key Infrastructure (PKI), two-party and n-party Diffie-Hellman schemes [10], can be used to design the security based model for mesh routers pattern.

Mesh clients Pattern: because the mesh clients are usually mobile and form the lower layer of communication with low input/output capability is the most challenging feature and reasonable level of security is required. Thus, in order to design the security based model for Mesh clients model, some cryptographic methods, such as symmetric cryptography (Block ciphers, Stream ciphers, Data Encryption Algorithm (DEA), The International Data Encryption Algorithm (IDEA) and threshold secret sharing models can be used to host the unique system requirement.

Mesh router & clients Pattern: the security based model for the Mesh router & clients pattern can be in between. In addition, as these three patterns belong to group communication models, the existing results for group key management [11, 12, 13] can be a great help to accomplish the development of security based model for the above three patterns.

C. Investigation of Security: The theoretical proof, investigation of security for the proposed security based model will be done at this step. There are two universal tools can be used for the simulation at this stage, Netsim, which is a great tool in the numerical computing area and network simulator-2.3, which is commonly used in the routing protocols and MAC protocols. Initial of all, the mathematical proof would be done to check the proposed model with aims of having common security issues, saying availability, integrity, authentication, confidentiality and coping well against the defined attack models to ensure the high level of security. Then by using Netsim, implementation would be carried out to measure the economic communication.

Scalability will be simulated to ensure the proposed security based model can cope well with the huge extendable networks. At the end, merits and demerits investigation would be provided to evaluate the developed security based model.

V. CONCLUSION

With more and more applications coming out, the destination of this promising technology, saying wireless mesh networks, will be well-performed, secure, and wide-spread wireless connection. To support the quality of large-scale deployment, it is rewarding and important to address the critical security model issue for wireless mesh networks. In this paper, we proposed scalable security based model for wireless mesh networks which aims to guarantee well performed security based model services and safety from potential attacks.

REFERENCE

[1]. Naouel Ben Salem and Jean-Pierre Hubaux, EPFL," securing wireless mesh networksIEEE wireless communication magazine .April 2006.

[2]. Umesh Kumar Singh, Shivlal Mewada, "Security Issues & Challenges in Wireless Mesh Networks", International Journal of Advanced Research in computer Science (IJARCS), Volume-2, No.5, pp(301-304), September-October 2011

[3]. Mewada Shivlal and Umesh Kumar Singh, "Performance Analysis of Secure Wireless Mesh Networks", Research Journal of Recent Sciences, Vol. 1(3), pp(80-85), March-2012.

[4]. Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani, "Distributed Architecture for Backbone Area Security of Wireless Mesh Networks", International Journal of Advanced Research in computer Science(IJARCS), Volume-2, No.3, pp(191-195), May-June 2011.

[5]. I. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Communications Magazine, vol. 43, no. 9, pp. 23–30, 2005.

[6]. R. Anderson and M. Kuhn. "Tamper Resistance - a Cautionary Note". In the USENIX Association in Proc. of the 2nd Workshop on Electronic Commerce, Oakland, California, Nov. 18-20, 1996.

[7]. Muhammad Shoaib Siddiqui, Choong Seon Hong, "Security Issues in Wireless Mesh Networks", Int. Conference on Multimedia and Ubiquitous Eng(2007), pp(717 - 722) IEEE Computer society.

[8]. A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. Swatt: Software-based attestation for embedded devices. In IEEE Symposium on Security and Privacy, 2004.

[9]. Y. Zhang, Y.; Fang. ARSA: An attack-resilient security architecture for multihop wireless mesh networks. In IEEE Journal on Selected Areas in Comm., vol 24, pages 1916–1928, Oct. 2006.

[10]. William Stallings, "Network Security Essentials", Third Edition, Prentice Hall, July 2006.

[11]. F Lee and S. Shieh, "Scalable and Lightweight Key Distribution for Secure Group Communications," International Journal of Network Management, 14:167-176, 2004.

[12]. Y. Fu, J. He, R. Wang and G. Li, "A key-chain-based keying scheme for many-to-many secure group comm,"ACM Transactions on Information and System Security, 2004, vol. 7(4), pp. 523 – 552.

[13]. K. Lu, Y. Qian and J. Hu, "A framework for distributed key management schemes in heterogeneous wireless sensor networks," 25thIEEE International Conference on Performance, Computing, and Comm. (IPCCC), pp. 513-519, Arizona, USA, April 10-12, 2006.

